



CVE-2016-4056

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2016-4056
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-23 21:59:00 UTC
Updated	2017-01-24 21:13:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the Backend component in TYPO3 6.2.x before 6.2.19 allows remote attackers to

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Typo3	Typo3	6.2	All	All	All
Application	Typo3	Typo3	6.2.0	alpha1	All	All
Application	Typo3	Typo3	6.2.0	alpha2	All	All
Application	Typo3	Typo3	6.2.0	alpha3	All	All
Application	Typo3	Typo3	6.2.0	beta1	All	All
Application	Typo3	Typo3	6.2.0	beta2	All	All
Application	Typo3	Typo3	6.2.0	beta3	All	All
Application	Typo3	Typo3	6.2.0	beta4	All	All
Application	Typo3	Typo3	6.2.0	beta5	All	All
Application	Typo3	Typo3	6.2.0	beta6	All	All
Application	Typo3	Typo3	6.2.0	beta7	All	All
Application	Typo3	Typo3	6.2.0	rc1	All	All
Application	Typo3	Typo3	6.2.0	rc2	All	All
Application	Typo3	Typo3	6.2.1	All	All	All
Application	Typo3	Typo3	6.2.10	All	All	All
Application	Typo3	Typo3	6.2.10	rc1	All	All
Application	Typo3	Typo3	6.2.11	All	All	All

Application	Typo3	Typo3	6.2.12	All	All	All
Application	Typo3	Typo3	6.2.13	All	All	All
Application	Typo3	Typo3	6.2.14	All	All	All
Application	Typo3	Typo3	6.2.15	All	All	All
Application	Typo3	Typo3	6.2.16	All	All	All
Application	Typo3	Typo3	6.2.17	All	All	All
Application	Typo3	Typo3	6.2.18	All	All	All
Application	Typo3	Typo3	6.2.2	All	All	All
Application	Typo3	Typo3	6.2.3	All	All	All
Application	Typo3	Typo3	6.2.4	All	All	All
Application	Typo3	Typo3	6.2.5	All	All	All
Application	Typo3	Typo3	6.2.6	All	All	All
Application	Typo3	Typo3	6.2.7	All	All	All
Application	Typo3	Typo3	6.2.8	All	All	All
Application	Typo3	Typo3	6.2.9	All	All	All
Application	Typo3	Typo3	6.2	All	All	All
Application	Typo3	Typo3	6.2.0	alpha1	All	All
Application	Typo3	Typo3	6.2.0	alpha2	All	All
Application	Typo3	Typo3	6.2.0	alpha3	All	All
Application	Typo3	Typo3	6.2.0	beta1	All	All
Application	Typo3	Typo3	6.2.0	beta2	All	All
Application	Typo3	Typo3	6.2.0	beta3	All	All
Application	Typo3	Typo3	6.2.0	beta4	All	All
Application	Typo3	Typo3	6.2.0	beta5	All	All
Application	Typo3	Typo3	6.2.0	beta6	All	All
Application	Typo3	Typo3	6.2.0	beta7	All	All
Application	Typo3	Typo3	6.2.0	rc1	All	All
Application	Typo3	Typo3	6.2.0	rc2	All	All
Application	Typo3	Typo3	6.2.1	All	All	All
Application	Typo3	Typo3	6.2.10	All	All	All
Application	Typo3	Typo3	6.2.10	rc1	All	All
Application	Typo3	Typo3	6.2.11	All	All	All
Application	Typo3	Typo3	6.2.12	All	All	All
Application	Typo3	Typo3	6.2.13	All	All	All
Application	Typo3	Typo3	6.2.14	All	All	All

Application	Typo3	Typo3	6.2.15	All	All	All
Application	Typo3	Typo3	6.2.16	All	All	All
Application	Typo3	Typo3	6.2.17	All	All	All
Application	Typo3	Typo3	6.2.18	All	All	All
Application	Typo3	Typo3	6.2.2	All	All	All
Application	Typo3	Typo3	6.2.3	All	All	All
Application	Typo3	Typo3	6.2.4	All	All	All
Application	Typo3	Typo3	6.2.5	All	All	All
Application	Typo3	Typo3	6.2.6	All	All	All
Application	Typo3	Typo3	6.2.7	All	All	All
Application	Typo3	Typo3	6.2.8	All	All	All
Application	Typo3	Typo3	6.2.9	All	All	All

References				
Reference	Source	Link	Tags	
CVE-2016-4056 - Stored Cross-Site Scripting in TYPO3 Bookmarks INTEGRITY Labs	MISC	labs.integrity.pt	Explo	
oss-security - Re: CVE Request: Stored Cross-Site Scripting in TYPO3 Bookmarks	MLIST	www.openwall.com	Maili	
Cross-Site Scripting in TYPO3 component Backend - - TYPO3 - The Enterprise Open Source CMS	CONFIRM	typo3.org	Patcl	
CVE Program record	CVE.ORG	www.cve.org	cano	
NVD vulnerability detail	NVD	nvd.nist.gov	cano	

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.